DogTag PKI Setup

Download Fedora 30 from osboxes.org

Link: https://sourceforge.net/projects/osboxes/files/v/vb/18-F-d/30/f30-64bit.7z/download

Set it up and start it up

Network: Dev Net Bridge

Setting up Fedora VM and Installation of Directory Server and PKI Packages

Reference: https://www.dogtagpki.org/wiki/Quick_Start#Installing_DS_and_PKI_Packages

Enable SSH

```
[root@fedora-ds ~]# systemctl enable sshd
Created symlink /etc/systemd/system/multi-user/target/wants/sshd.service -> /usr/lib/systemd/system/sshd.
service.
[root@fedora-ds ~]# systemctl start sshd
```

Configure hostname

```
[root@localhost ~]# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 200.168.18.164  netmask 255.255.255.0  broadcast 200.168.18.255
        inet6 fe80::3759:1e99:1c48:4eec  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:80:5f:fc  txqueuelen 1000  (Ethernet)
        RX packets 832959  bytes 1220179763 (1.1 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 117264  bytes 7872003 (7.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 52  bytes 4253 (4.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 52  bytes 4253 (4.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@localhost ~]# echo "200.168.18.164 fedora-ds.klass.dev" >> /etc/hosts
[root@localhost ~]# cat /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
200.168.18.164 fedora-ds.klass.dev
[root@localhost ~]# echo "fedora-ds.klass.dev" > /etc/hostname
[root@localhost ~]# shutdown -r now
```

Install directory server and dogtag-pki packages:

```
[root@fedora-ds ~]# yum install 389-ds-base dogtag-pki
Last metadata expiration check: 0:03:03 ago on Wed 12 Jun 2019 02:46:09 PM.
...
[See Appendix A]
...
Complete!
```

Install directory server:

```
[root@fedora-ds ~]# setup-ds.pl

==============================================================================
This program will set up the 389 Directory Server.

It is recommended that you have "root" privilege to set up the software.
Tips for using this  program:
  - Press "Enter" to choose the default and go to the next screen
  - Type "Control-B" or the word "back" then "Enter" to go back to the previous screen
  - Type "Control-C" to cancel the setup program

Would you like to continue with set up? [yes]: yes

==============================================================================
Choose a setup type:

   1. Express
       Allows you to quickly set up the servers using the most
       common options and pre-defined defaults. Useful for quick
       evaluation of the products.

   2. Typical
       Allows you to specify common defaults and options.

   3. Custom
       Allows you to specify more advanced options. This is
       recommended for experienced server administrators only.

To accept the default shown in brackets, press the Enter key.

Choose a setup type [2]: 1

==============================================================================
Certain directory server operations require an administrative user.
This user is referred to as the Directory Manager and typically has a
bind Distinguished Name (DN) of cn=Directory Manager.
You will also be prompted for the password for this user.  The password must
be at least 8 characters long, and contain no spaces.
Press Control-B or type the word "back", then Enter to back up and start over.

Directory Manager DN [cn=Directory Manager]:
Password: password
Password (confirm): password
Your new DS instance 'fedora-ds' was successfully created.
Exiting . . .
Log file is '/tmp/setuplXFbjh.log'
```

Create CA Subsystem

```
[root@fedora-ds ~]# pkispawn

IMPORTANT:

    Interactive installation currently only exists for very basic deployments!

    For example, deployments intent upon using advanced features such as:

        * Cloning,
        * Elliptic Curve Cryptography (ECC),
        * External CA,
        * Hardware Security Module (HSM),
        * Subordinate CA,
        * etc.,

    must provide the necessary override parameters in a separate
    configuration file.
    Run 'man pkispawn' for details.

Subsystem (CA/KRA/OCSP/TKS/TPS) [CA]: CA

Tomcat:
  Instance [pki-tomcat]:
  HTTP port [8080]:
  Secure HTTP port [8443]:
  AJP port [8009]:
  Management port [8005]:

Administrator:
  Username [caadmin]:
  Password: password
  Verify password: password
  Import certificate (Yes/No) [N]?
  Export certificate to [/root/.dogtag/pki-tomcat/ca_admin.cert]:

Directory Server:
  Hostname [fedora-ds.klass.dev]:
  Use a secure LDAPS connection (Yes/No/Quit) [N]?
  LDAP Port [389]:
  Bind DN [cn=Directory Manager]:
  Password: password
  Base DN [o=pki-tomcat-CA]:

Security Domain:
  Name [klass.dev Security Domain]:

Begin installation (Yes/No/Quit)? yes

Log file: /var/log/pki/pki-ca-spawn.20190613224457.log
Installing CA into /var/lib/pki/pki-tomcat.
Storing deployment configuration into /etc/sysconfig/pki/tomcat/pki-tomcat/ca/deployment.cfg.
Notice: Trust flag u is set automatically if the private key is present.
The unit files have no installation config (WantedBy=, RequiredBy=, Also=,
Alias= settings in the [Install] section, and DefaultInstance= for template
units). This means they are not meant to be enabled using systemctl.

Possible reasons for having this kind of units are:
• A unit may be statically enabled by being symlinked from another unit's
  .wants/ or .requires/ directory.
• A unit's purpose may be to act as a helper for some other unit which has
  a requirement dependency on it.
• A unit may be started when needed via activation (socket, path, timer,
  D-Bus, udev, scripted systemctl call, ...).
• In case of template units, the unit is meant to be enabled with some
  instance name specified.

    ==========================================================================
                                INSTALLATION SUMMARY
    ==========================================================================

      Administrator's username:             caadmin
      Administrator's PKCS #12 file:
            /root/.dogtag/pki-tomcat/ca_admin_cert.p12

      This CA subsystem of the 'pki-tomcat' instance
      has FIPS mode enabled on this operating system.

      REMINDER:  Don't forget to update the appropriate FIPS
                 algorithms in server.xml in the 'pki-tomcat' instance.

      To check the status of the subsystem:
            systemctl status pki-tomcatd@pki-tomcat.service

      To restart the subsystem:
            systemctl restart pki-tomcatd@pki-tomcat.service

      The URL for the subsystem is:
            https://fedora-ds.klass.dev:8443/ca
      PKI instances will be enabled upon system boot

    ==========================================================================
```

Accessing CA Admin Page from Host Machine

The CA Agent page can be accessed by using the default admin credentials generated from the CA installation steps. It is also possible to create new CA Agent accounts and use that instead. To do that, follow instructions detailed here: https://www.dogtagpki.org/wiki/CA_Agent_Setup

Depending on whether a new CA Agent account was set up:

Copy the CA Agent private key and cert

```
[root@fedora-ds ~]# scp /root/.dogtag/pki-tomcat/new_ca_agent_cert.p12 hostuser@hostmachineip:~/
```

Or

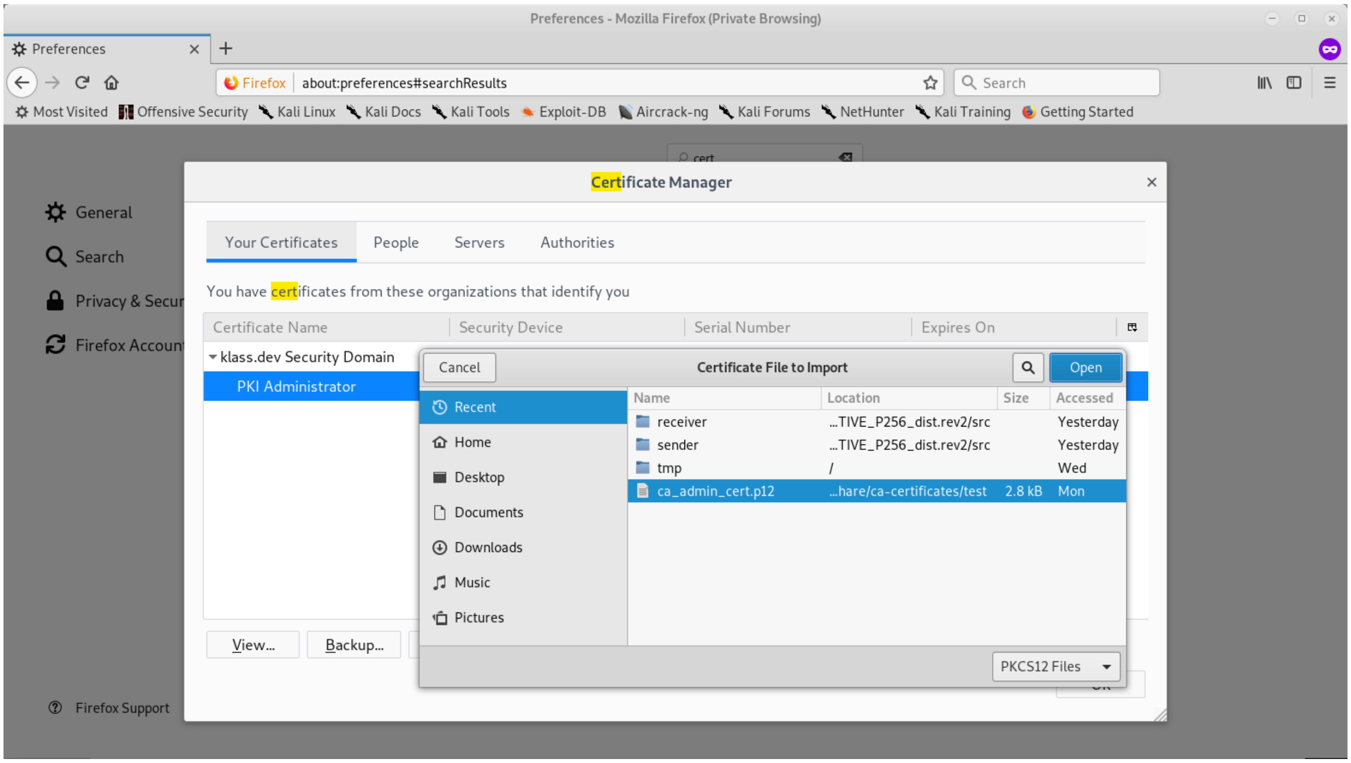
Copy the default admin private key and cert

```
[root@fedora-ds ~]# scp /root/.dogtag/pki-tomcat/ca_admin_cert.p12 hostuser@hostmachineip:~/
```

Obtain and copy the CA Signing certificate

```
[root@fedora-ds ~]# pki-server cert-export ca_signing --cert-file ca_signing.crt
[root@fedora-ds ~]# ls
anaconda-ks.cfg  ca_signing.crt
[root@fedora-ds ~]# scp ca_signing.crt hostuser@hostmachineip:~/
```

Add the CA Agent credentials and Trust the CA Certificate in the browser:



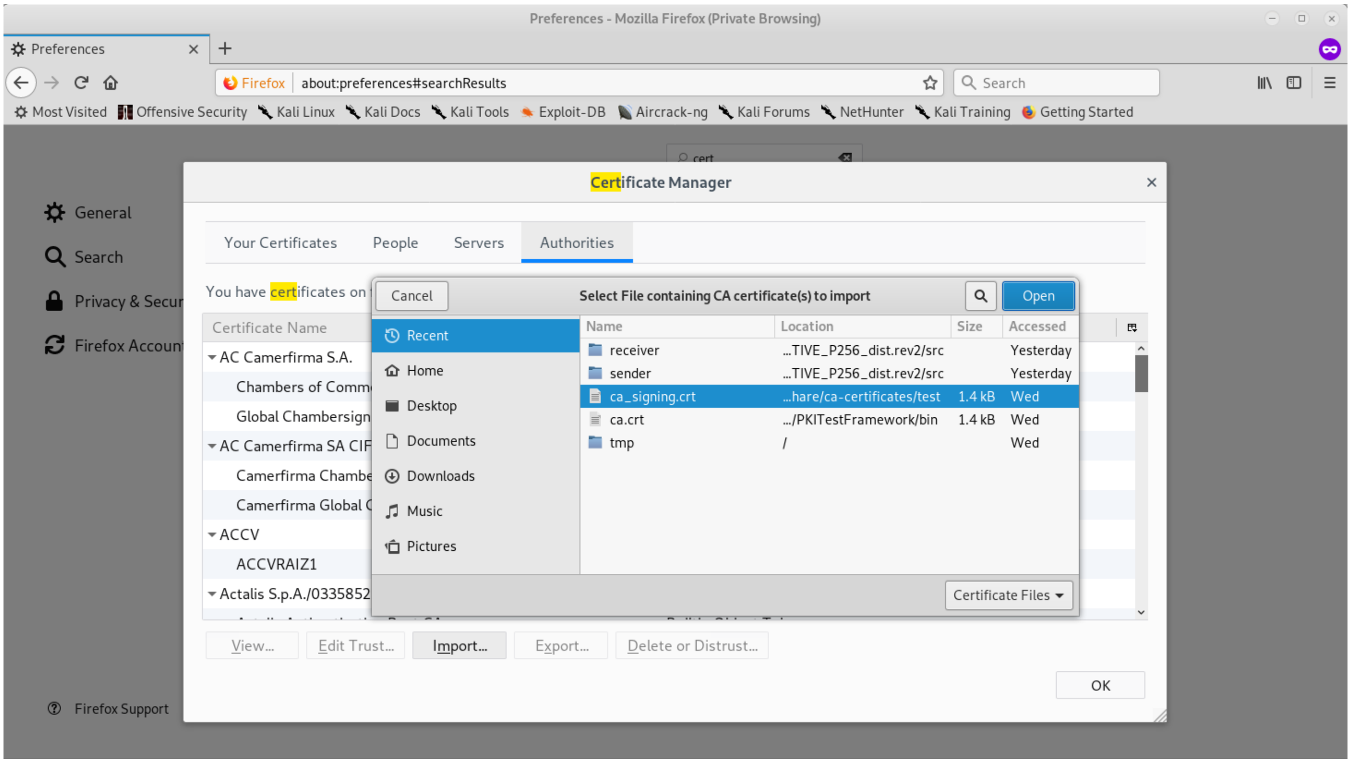
Certificate Manager

You have certificates from these organizations that identify you

Certificate Name	Security Device	Serial Number	Expires On
klass.dev Security Domain			
PKI Administrator			

Certificate File to Import

Name	Location	Size	Accessed
receiver	...TIVE_P256_dist.rev2/src		Yesterday
sender	...TIVE_P256_dist.rev2/src		Yesterday
tmp	/		Wed
ca_admin_cert.p12	...hare/ca-certificates/test	2.8 kB	Mon



Certificate Manager

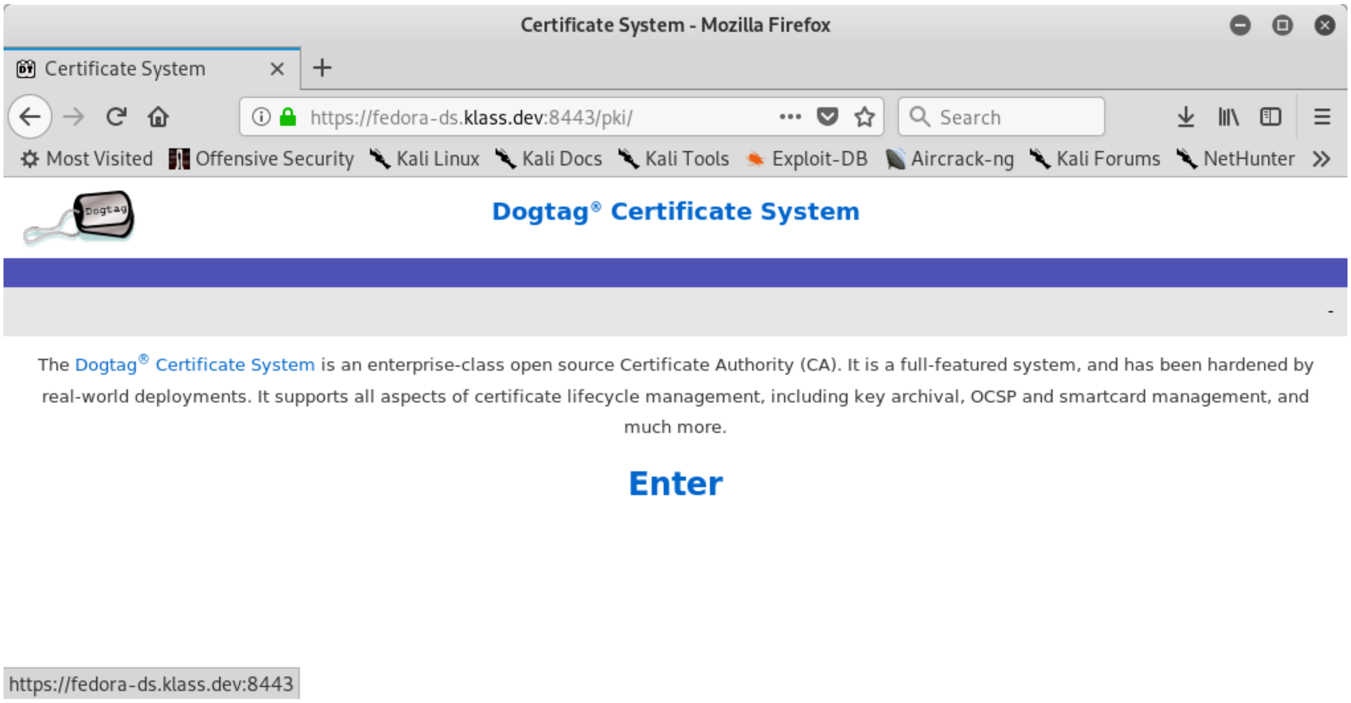
You have certificates on

Certificate Name
AC Camerfirma S.A.
Chambers of Comm
Global Chambersign
AC Camerfirma SA CIF
Camerfirma Chambe
Camerfirma Global C
ACCV
ACCVRAIZ1
Actalis S.p.A./0335852

Select File containing CA certificate(s) to import

Name	Location	Size	Accessed
receiver	...TIVE_P256_dist.rev2/src		Yesterday
sender	...TIVE_P256_dist.rev2/src		Yesterday
ca_signing.crt	...hare/ca-certificates/test	1.4 kB	Wed
ca.crt	.../PKITestFramework/bin	1.4 kB	Wed
tmp	/		Wed

CA Admin Page is now accessible



Certificate System - Mozilla Firefox

https://fedora-ds.klass.dev:8443/pki/

Dogtag® Certificate System

The Dogtag® Certificate System is an enterprise-class open source Certificate Authority (CA). It is a full-featured system, and has been hardened by real-world deployments. It supports all aspects of certificate lifecycle management, including key archival, OCSP and smartcard management, and much more.

Setting up a Peer

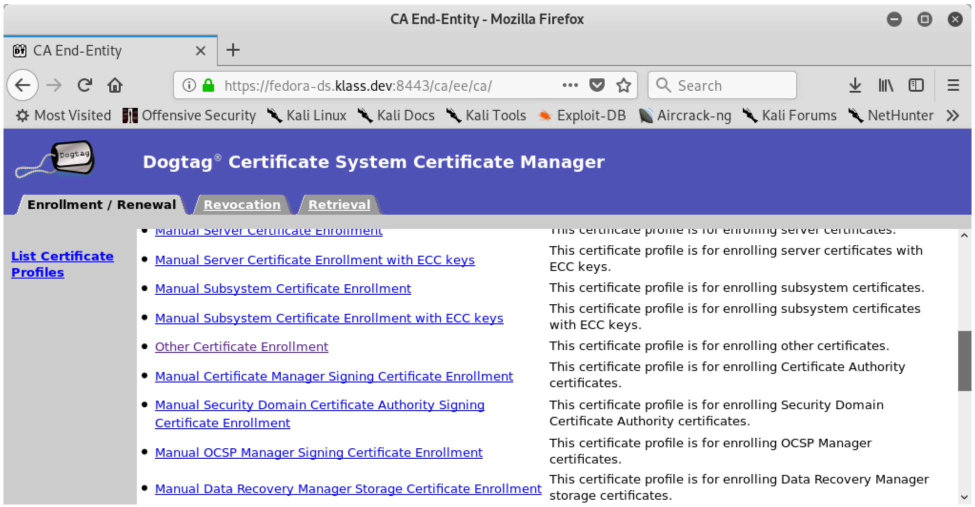
Generate Peer Key and Certificate Signing Request

```
user@hostmachine:/tmp$ openssl req -new -newkey rsa:2048 -nodes -keyout peer.key -out peer.csr
Generating a RSA private key
............................+++++
.+++++
writing new private key to 'peer.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:SG
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:Peer 1 Example
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
user@hostmachine:/tmp$ cat peer.csr
-----BEGIN CERTIFICATE REQUEST-----
-----BEGIN CERTIFICATE REQUEST-----
MIICozCCAYsCAQAwXjELMAkGA1UEBhMCU0cxEzARBgNVBAgMClNvbWUtU3RhdGUx
ITAfBgNVBAoMGEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDEXMBUGA1UEAwwOUGVl
ciAxIEV4YW1wbGUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCVeCmL
xAy30j19u+PxU9NiHXnQIXvSh1aDqDl/ugEYDLL3AS5mtSu/Zg8yclC7+9PzDgAN
o4qSVlHvRtuYdpykD0B66BtrjIgYoGCeV7i4m3xJLePGP47kx758ZAQMEzfwBtM+
VJVehHdArjfcRJN8HwpjGbbR+FkRk4Trv1DTkeZ35egTAHro/TuCKB5Y/EeoE+CS
ios2spWiH5AJDYV9mY/MnKpFYYCVtMIAtJ9mjW0NXmoczhG08PH1+C4DX2pLVvj7
s+mSho73i6guKwLUBXZ54cAucIw/9hiNcgA9y+7ESPO4tjTGsnrEqAdBTqeAcLV5
lvJFwj7EitBxzBZZAgMBAAGgADANBgkqhkiG9w0BAQsFAAOCAQEAOGhTzvDPobEO
0mcVm2eGBf+MpcX1bzy4WLMRq7s2/izzxfeHx/EQjjFHxFw1hlbaXZFQWcTxXK+F
07yhvlHggPwCKmUkY/ale9eNlqdaRYrkiC2INn1KePgqfyyhoW1wJktL+nTMUOSk
TiHamGY0Lm/uRNI86zIroNs00eDFpesOMdsHNe9HCqp7rjpYaZactvgLapb+1Olj
Vba/+0xYIsJaSBHlGS4rYdnFgCk7fsoC4ppbjobUifxgECQXYlgPmjC+ANBt8Tft
ZSbY5y49L/hBYCgRmcyKXHoELdQFp4ln/dMhBA0F/5YzabIa1a/2G8qaUPkoT4BF
rHcNQQ3UAw==
-----END CERTIFICATE REQUEST-----
```

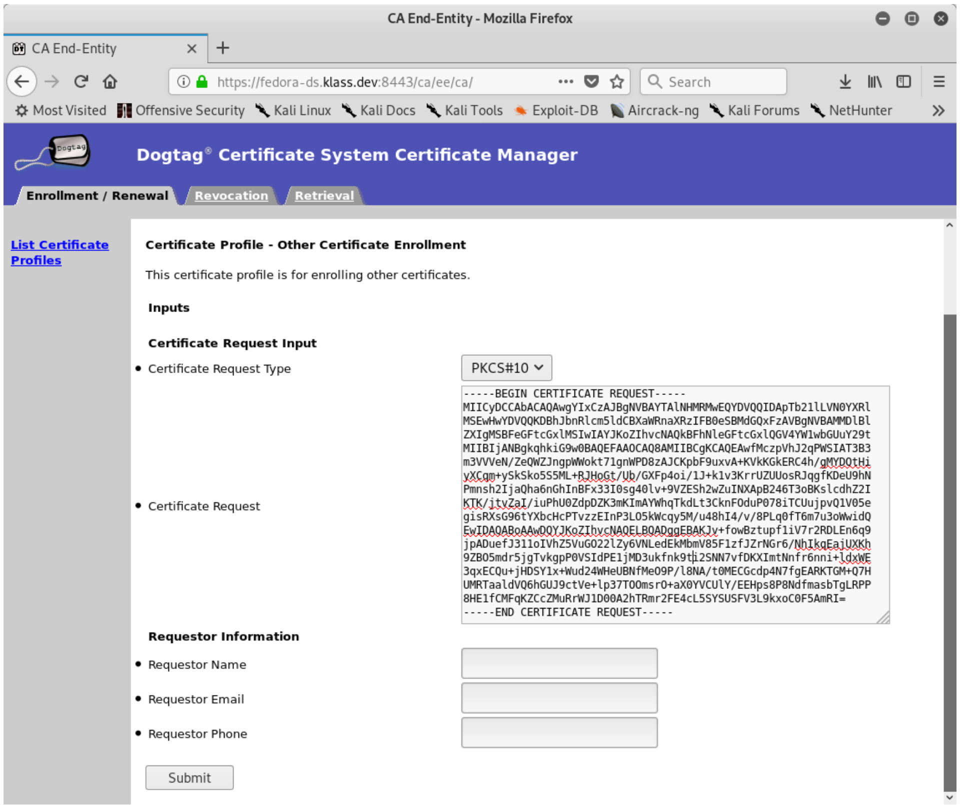
Submit A Certificate Signing Request:

Click on "Other Certificate Enrollment":



- Manual Server Certificate Enrollment — This certificate profile is for enrolling server certificates.
- Manual Server Certificate Enrollment with ECC keys — This certificate profile is for enrolling server certificates with ECC keys.
- Manual Subsystem Certificate Enrollment — This certificate profile is for enrolling subsystem certificates.
- Manual Subsystem Certificate Enrollment with ECC keys — This certificate profile is for enrolling subsystem certificates with ECC keys.
- Other Certificate Enrollment — This certificate profile is for enrolling other certificates.
- Manual Certificate Manager Signing Certificate Enrollment — This certificate profile is for enrolling Certificate Authority certificates.
- Manual Security Domain Certificate Authority Signing Certificate Enrollment — This certificate profile is for enrolling Security Domain Certificate Authority certificates.
- Manual OCSP Manager Signing Certificate Enrollment — This certificate profile is for enrolling OCSP Manager certificates.
- Manual Data Recovery Manager Storage Certificate Enrollment — This certificate profile is for enrolling Data Recovery Manager storage certificates.

Copy and paste the CSR contents then click submit.



Certificate Profile - Other Certificate Enrollment

This certificate profile is for enrolling other certificates.

Inputs

Certificate Request Input

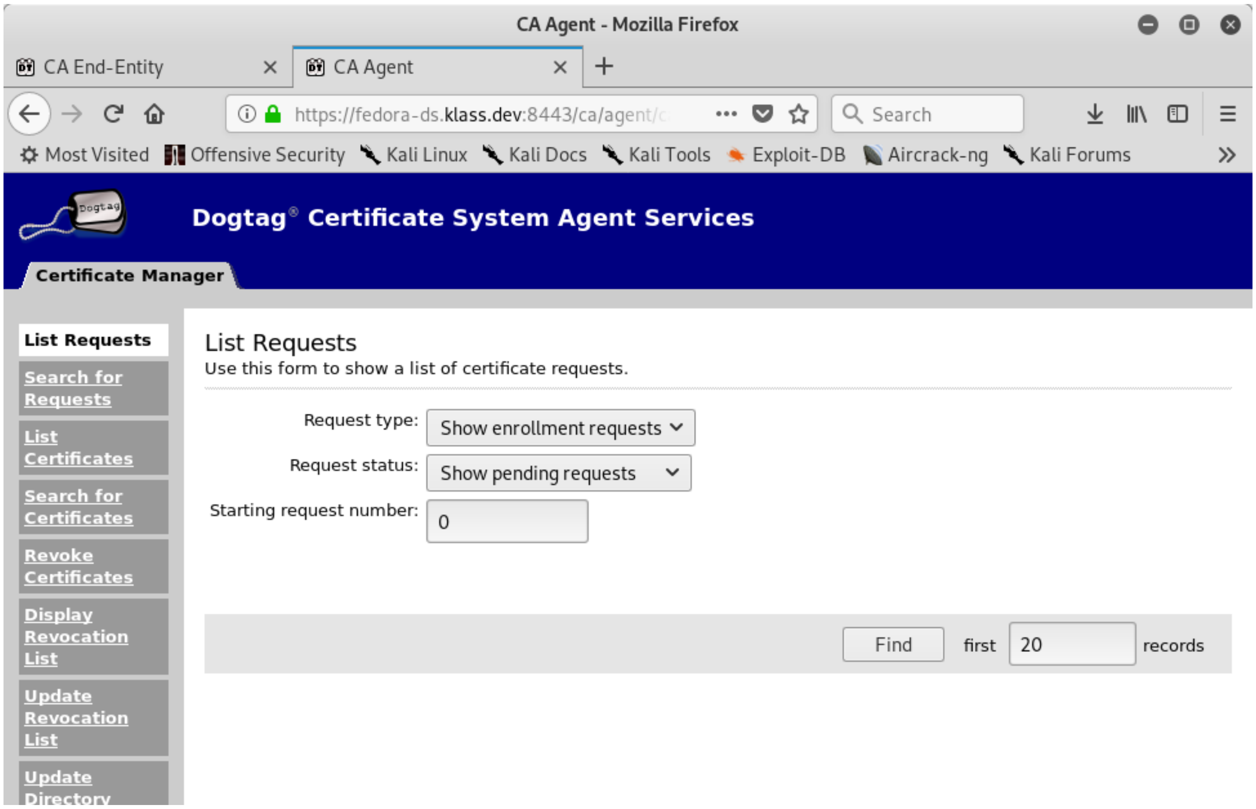
- Certificate Request Type: PKCS#10
- Certificate Request:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICyDCCAbACAQAwgYIxCzAJBgNVBAYTAlNHMRMwEQYDVQQIDApTb21lLVN0YXRl
MSEwHwYDVQQKDBhJbnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQxFzAVBgNVBAMMDlBl
ZXIgMSBFeGFtcGxlMSIwIAYJKoZIhvcNAQkBFhNleGFtcGxlQGV4YW1wbGUuY29t
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwfMczpVhJ2qPWSIAT3B3
m3VVVeN/ZeQWZJngpWWokt71gnWPD8zAJCKpbF9uxvA+KVkKGkERC4h/gMYDQtHi
yXCqm+ySkSko5S5ML+RJHoGt/Ub/GXFp4oi/1J+k1v3KrrUZUUosRJqgfKDeU9hN
Pmnsh2IjaQha6nGhInBFx33I0sg40lv+9VZESh2wZuINXApB246T3oBKslcdhZ2I
KTK/jtvZaI/iuPhU0ZdpDZK3mKImAYWhqTkdLt3CknFOduP078iTCUujpvQ1V05e
gisRXsG96tYXbcHcPTvzzEInP3LO5kWcqy5M/u48hI4/v/8PLq0fT6m7u3oWwidQ
EwIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBAKJv+fowBztupf1iV7r2RDLEn6q9
jpADuefJ311oIVhZ5VuGO22lZy6VNLedEkMbmV85F1zfJZrNGr6/NhIkqEajUXKh
9ZBO5mdr5jgTvkgpP0VSIdPE1jMD3ukfnk9ti2SNN7vfDKXImtNnfr6nni+ldxWE
3qxECQu+jHDSY1x+Wud24WHeUBNfMeO9P/l8NA/t0MECGcdp4N7fgEARKTGM+Q7H
UMRTaaldVQ6hGUJ9ctVe+lp37TOOmsrO+aX0YVCUlY/EEHps8P8NdfmasbTgLRPP
8HE1fCMFqKZCcZMuRrWJ1D00A2hTRmr2FE4cL5SYSUSFV3L9kxoC0F5AmRI=
-----END CERTIFICATE REQUEST-----
```

Requestor Information

- Requestor Name
- Requestor Email
- Requestor Phone

Accept the certificate signing request



List Requests

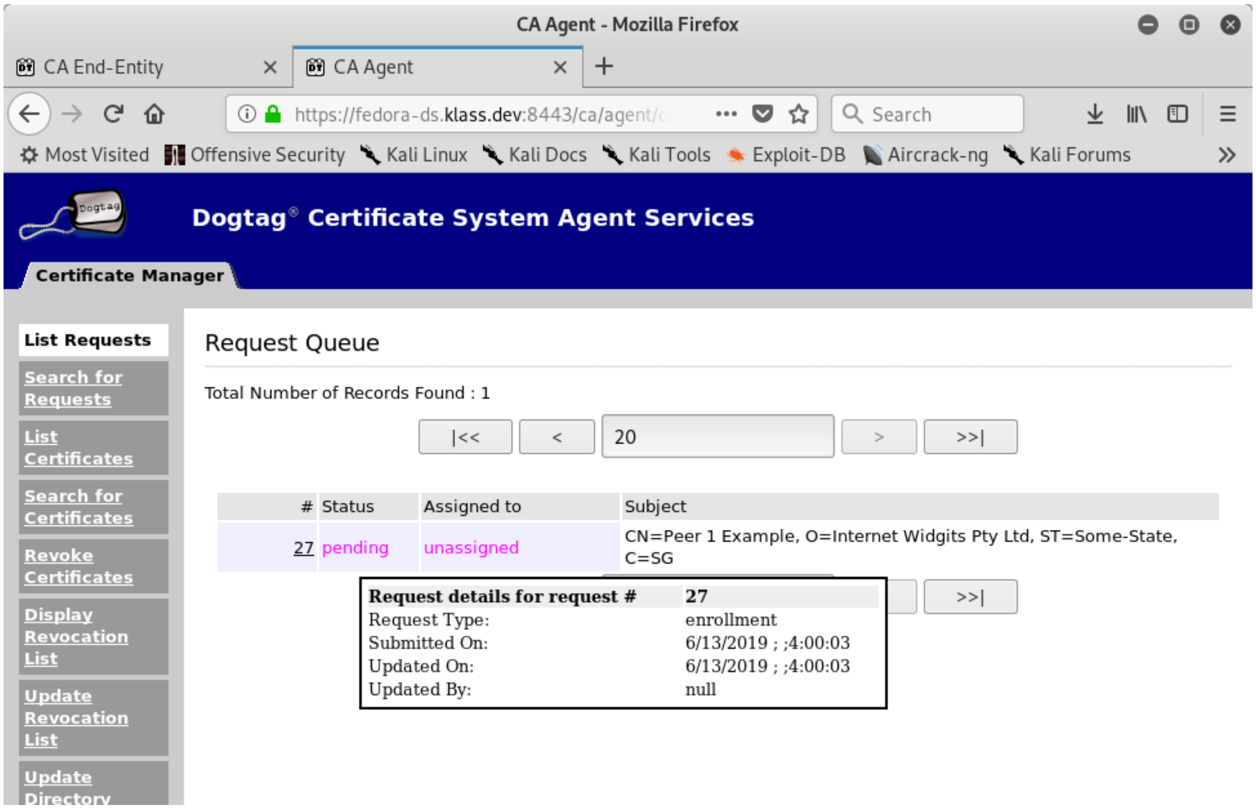
Use this form to show a list of certificate requests.

Request type: Show enrollment requests

Request status: Show pending requests

Starting request number: 0

Find first 20 records



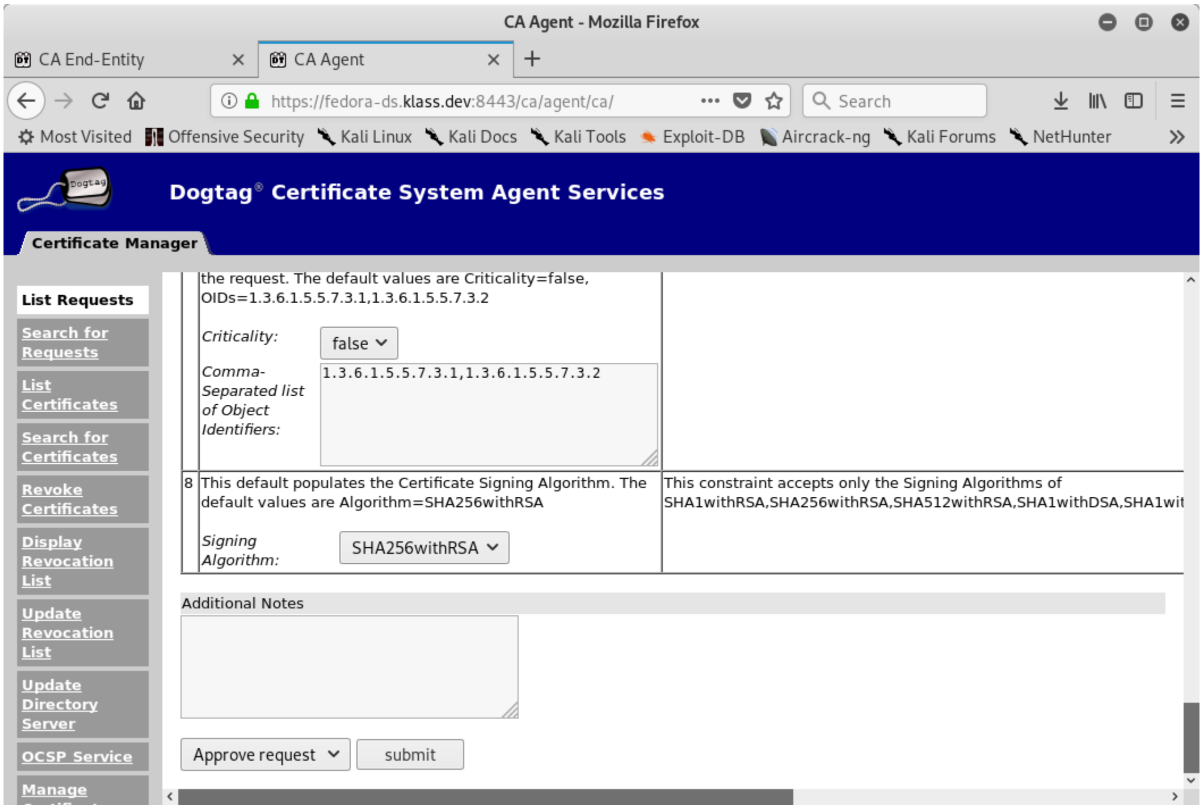
Request Queue

Total Number of Records Found : 1

20

#	Status	Assigned to	Subject
27	pending	unassigned	CN=Peer 1 Example, O=Internet Widgits Pty Ltd, ST=Some-State, C=SG

Request details for request #	**27**
Request Type:	enrollment
Submitted On:	6/13/2019 ; ;4:00:03
Updated On:	6/13/2019 ; ;4:00:03
Updated By:	null



the request. The default values are Criticality=false, OIDs=1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2

Criticality: false

Comma-Separated list of Object Identifiers: 1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2

8 This default populates the Certificate Signing Algorithm. The default values are Algorithm=SHA256withRSA

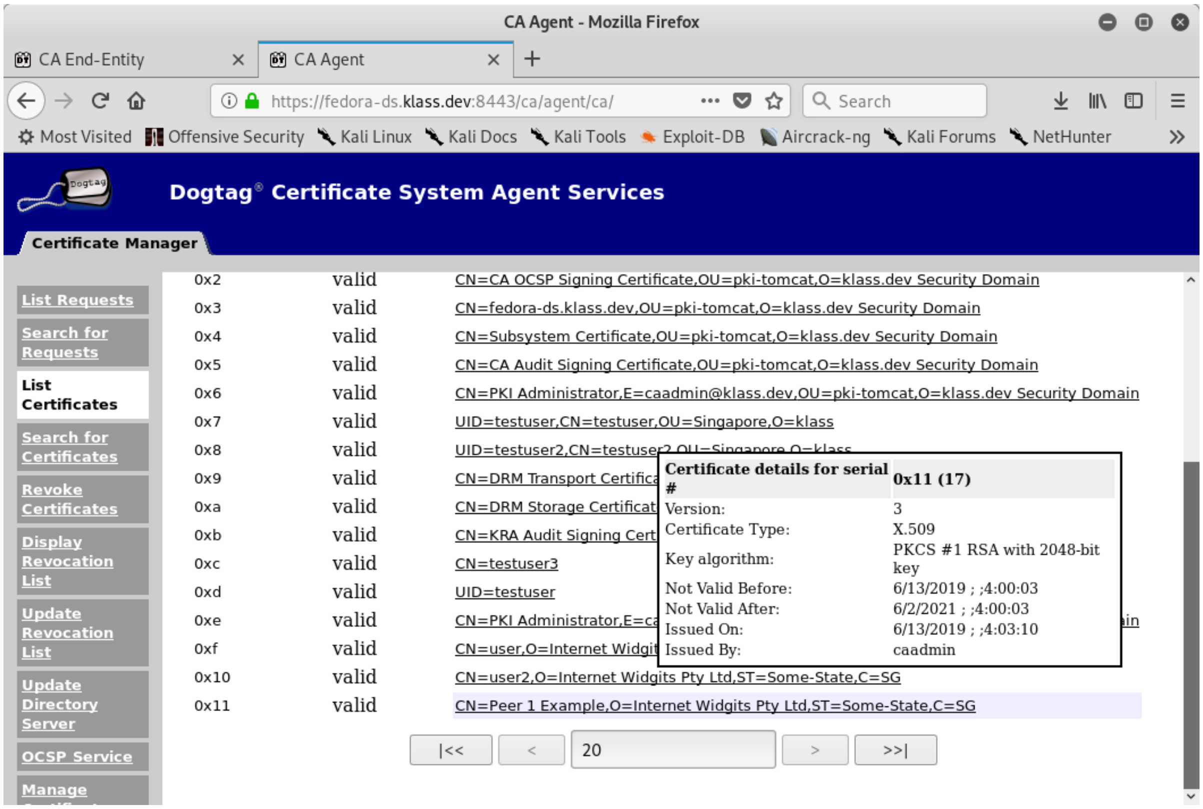
Signing Algorithm: SHA256withRSA

This constraint accepts only the Signing Algorithms of SHA1withRSA,SHA256withRSA,SHA512withRSA,SHA1withDSA,SHA1wit

Additional Notes

Approve request — submit

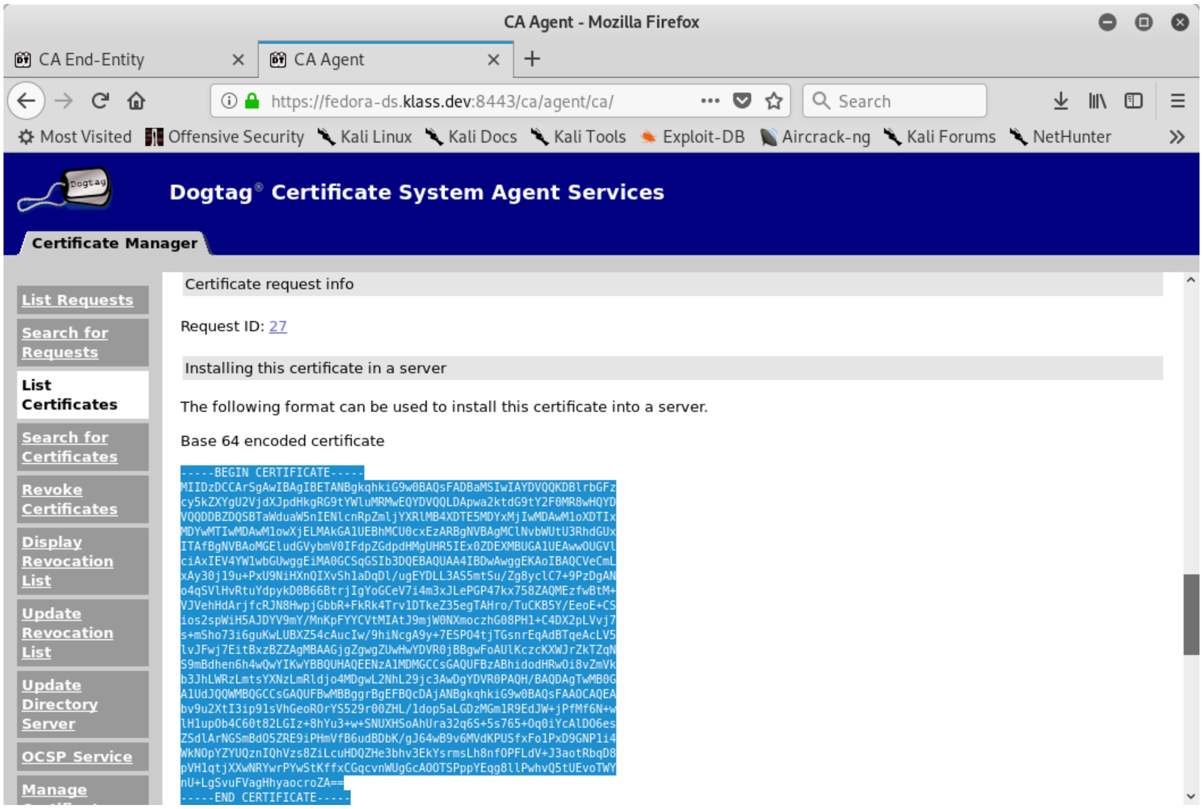
Check that the certificate is now in the system:



0x2	valid	CN=CA OCSP Signing Certificate,OU=pki-tomcat,O=klass.dev Security Domain
0x3	valid	CN=fedora-ds.klass.dev,OU=pki-tomcat,O=klass.dev Security Domain
0x4	valid	CN=Subsystem Certificate,OU=pki-tomcat,O=klass.dev Security Domain
0x5	valid	CN=CA Audit Signing Certificate,OU=pki-tomcat,O=klass.dev Security Domain
0x6	valid	CN=PKI Administrator,E=caadmin@klass.dev,OU=pki-tomcat,O=klass.dev Security Domain
0x7	valid	UID=testuser,CN=testuser,OU=Singapore,O=klass
0x8	valid	UID=testuser2,CN=testuser2,OU=Singapore,O=klass
0x9	valid	CN=DRM Transport Certifica
0xa	valid	CN=DRM Storage Certificat
0xb	valid	CN=KRA Audit Signing Cert
0xc	valid	CN=testuser3
0xd	valid	UID=testuser
0xe	valid	CN=PKI Administrator,E=ca ain
0xf	valid	CN=user,O=Internet Widgit
0x10	valid	CN=user2,O=Internet Widgits Pty Ltd,ST=Some-State,C=SG
0x11	valid	CN=Peer 1 Example,O=Internet Widgits Pty Ltd,ST=Some-State,C=SG

Certificate details for serial #	0x11 (17)
Version:	3
Certificate Type:	X.509
Key algorithm:	PKCS #1 RSA with 2048-bit key
Not Valid Before:	6/13/2019 ; ;4:00:03
Not Valid After:	6/2/2021 ; ;4:00:03
Issued On:	6/13/2019 ; ;4:03:10
Issued By:	caadmin

20



Certificate request info

Request ID: 27

Installing this certificate in a server

The following format can be used to install this certificate into a server.

Base 64 encoded certificate

```
-----BEGIN CERTIFICATE-----
MIIDzDCCArSgAwIBAgIBETANBgkqhkiG9w0BAQsFADBaMSIwIAYDVQQKDBlrbGFz
cy5kZXYgU2VjdXJpdHkgRG9tYWluMRMwEQYDVQQLDApwa2ktdG9tY2F0MR8wHQYD
VQQDDBZDQSBTaWduaW5nIENlcnRpZmljYXRlMB4XDTE5MDYxMjIwMDAwM1oXDTIx
MDYwMTIwMDAwM1owXjELMAkGA1UEBhMCU0cxEzARBgNVBAgMClNvbWUtU3RhdGUx
ITAfBgNVBAoMGEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDEXMBUGA1UEAwwOUGVl
ciAxIEV4YW1wbGUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCVeCmL
xAy30j19u+PxU9NiHXnQIXvSh1aDqDl/ugEYDLL3AS5mtSu/Zg8yclC7+9PzDgAN
o4qSVlHvRtuYdpykD0B66BtrjIgYoGCeV7i4m3xJLePGP47kx758ZAQMEzfwBtM+
VJVehHdArjfcRJN8HwpjGbbR+FkRk4Trv1DTkeZ35egTAHro/TuCKB5Y/EeoE+CS
ios2spWiH5AJDYV9mY/MnKpFYYCVtMIAtJ9mjW0NXmoczhG08PH1+C4DX2pLVvj7
s+mSho73i6guKwLUBXZ54cAucIw/9hiNcgA9y+7ESPO4tjTGsnrEqAdBTqeAcLV5
lvJFwj7EitBxzBZZAgMBAAGjgZgwgZUwHwYDVR0jBBgwFoAUlKczcKXWJrZkTZqN
S9mBdhen6h4wQwYIKwYBBQUHAQEENzA1MDMGCCsGAQUFBzABhidodHRwOi8vZmVk
b3JhLWRzLmtsYXNzLmRldjo4MDgwL2NhL29jc3AwDgYDVR0PAQH/BAQDAgTwMB0G
A1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjANBgkqhkiG9w0BAQsFAAOCAQEA
bv9u2XtI3ip91sVhGeoROrYS529r00ZHL/1dop5aLGDzMGm1R9EdJW+jPfMf6N+w
lH1upOb4C60t82LGIz+8hYu3+w+SNUXHSoAhUra32q6S+5s765+Oq0iYcAlDO6es
ZSdlArNGSmBdO5ZRE9iPHmVfB6udBDbK/gJ64wB9v6MVdKPUSfxFo1PxD9GNP1i4
WkNOpYZYUQznIQhVzs8ZiLcuHDQZHe3bhv3EkYsrmsLh8nfOPFLdV+J3aotRbqD8
pVH1qtjXXwNRYwrPYwStKffxCGqcvnWUgGcAOOTSPppYEqg8llPwhvQ5tUEvoTWY
nU+LgSvuFVagHhyaocroZA==
-----END CERTIFICATE-----
```

Retrieve the certificate via CLI

```
[osboxes@fedora-ds ~]$ pki ca-cert-find
----------------
17 entries found
----------------
...
...
  Serial Number: 0x11
  Subject DN: CN=Peer 1 Example,O=Internet Widgits Pty Ltd,ST=Some-State,C=SG
  Issuer DN: CN=CA Signing Certificate,OU=pki-tomcat,O=klass.dev Security Domain
  Status: VALID
  Type: X.509 version 3
  Key Algorithm: PKCS #1 RSA with 2048-bit key
  Not Valid Before: Wed Jun 12 16:00:03 EDT 2019
  Not Valid After: Tue Jun 01 16:00:03 EDT 2021
  Issued On: Wed Jun 12 16:03:10 EDT 2019
  Issued By: caadmin
-----------------------------
Number of entries returned 17
-----------------------------
[osboxes@fedora-ds ~]$ pki ca-cert-show 0x11 --output peer.crt
------------------
Certificate "0x11"
------------------
  Serial Number: 0x11
  Subject DN: CN=Peer 1 Example,O=Internet Widgits Pty Ltd,ST=Some-State,C=SG
  Issuer DN: CN=CA Signing Certificate,OU=pki-tomcat,O=klass.dev Security Domain
  Status: VALID
  Not Valid Before: Wed Jun 12 16:00:03 EDT 2019
  Not Valid After: Tue Jun 01 16:00:03 EDT 2021
[osboxes@fedora-ds ~]$ cat peer.crt
-----BEGIN CERTIFICATE-----
MIIDzDCCArSgAwIBAgIBETANBgkqhkiG9w0BAQsFADBaMSIwIAYDVQQKDBlrbGFz
cy5kZXYgU2VjdXJpdHkgRG9tYWluMRMwEQYDVQQLDApwa2ktdG9tY2F0MR8wHQYD
VQQDDBZDQSBTaWduaW5nIENlcnRpZmljYXRlMB4XDTE5MDYxMjIwMDAwM1oXDTIx
MDYwMTIwMDAwM1owXjELMAkGA1UEBhMCU0cxEzARBgNVBAgMClNvbWUtU3RhdGUx
ITAfBgNVBAoMGEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDEXMBUGA1UEAwwOUGVl
ciAxIEV4YW1wbGUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCVeCmL
xAy30j19u+PxU9NiHXnQIXvSh1aDqDl/ugEYDLL3AS5mtSu/Zg8yclC7+9PzDgAN
o4qSVlHvRtuYdpykD0B66BtrjIgYoGCeV7i4m3xJLePGP47kx758ZAQMEzfwBtM+
VJVehHdArjfcRJN8HwpjGbbR+FkRk4Trv1DTkeZ35egTAHro/TuCKB5Y/EeoE+CS
ios2spWiH5AJDYV9mY/MnKpFYYCVtMIAtJ9mjW0NXmoczhG08PH1+C4DX2pLVvj7
s+mSho73i6guKwLUBXZ54cAucIw/9hiNcgA9y+7ESPO4tjTGsnrEqAdBTqeAcLV5
lvJFwj7EitBxzBZZAgMBAAGjgZgwgZUwHwYDVR0jBBgwFoAUlKczcKXWJrZkTZqN
S9mBdhen6h4wQwYIKwYBBQUHAQEENzA1MDMGCCsGAQUFBzABhidodHRwOi8vZmVk
b3JhLWRzLmtsYXNzLmRldjo4MDgwL2NhL29jc3AwDgYDVR0PAQH/BAQDAgTwMB0G
A1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjANBgkqhkiG9w0BAQsFAAOCAQEA
bv9u2XtI3ip91sVhGeoROrYS529r00ZHL/1dop5aLGDzMGm1R9EdJW+jPfMf6N+w
lH1upOb4C60t82LGIz+8hYu3+w+SNUXHSoAhUra32q6S+5s765+Oq0iYcAlDO6es
ZSdlArNGSmBdO5ZRE9iPHmVfB6udBDbK/gJ64wB9v6MVdKPUSfxFo1PxD9GNP1i4
WkNOpYZYUQznIQhVzs8ZiLcuHDQZHe3bhv3EkYsrmsLh8nfOPFLdV+J3aotRbqD8
pVH1qtjXXwNRYwrPYwStKffxCGqcvnWUgGcAOOTSPppYEqg8llPwhvQ5tUEvoTWY
nU+LgSvuFVagHhyaocroZA==
-----END CERTIFICATE-----
```

Verifying the certificate's OCSP URI and certificate validation using OCSP:

```
user@hostmachine:/tmp$ openssl x509 -noout -ocsp_uri -in peer.crt
http://fedora-ds.klass.dev:8080/ca/ocsp
user@hostmachine:/tmp$ openssl ocsp -issuer ca_signing.crt -cert peer.crt -text -url http://fedora-ds.klass.dev:
8080/ca/ocsp
OCSP Request Data:
    Version: 1 (0x0)
    Requestor List:
        Certificate ID:
          Hash Algorithm: sha1
          Issuer Name Hash: 48F30F7A29DDBF0E0FF4FF8BBD92BC897BDFDCAD
          Issuer Key Hash: 94A73370A5D626B6644D9A8D4BD9817617A7EA1E
          Serial Number: 11
    Request Extensions:
        OCSP Nonce:
            04107A245776F7D27E0EE97A205C4CC0D612
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: O = klass.dev Security Domain, OU = pki-tomcat, CN = CA OCSP Signing Certificate
    Produced At: Jun 12 20:22:11 2019 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 48F30F7A29DDBF0E0FF4FF8BBD92BC897BDFDCAD
      Issuer Key Hash: 94A73370A5D626B6644D9A8D4BD9817617A7EA1E
      Serial Number: 11
    Cert Status: good
    This Update: Jun 12 20:22:11 2019 GMT

    Response Extensions:
        OCSP Nonce:
            04107A245776F7D27E0EE97A205C4CC0D612
    Signature Algorithm: sha256WithRSAEncryption
         cc:62:aa:e0:a9:cc:3e:87:31:d4:4b:a9:c9:7a:29:92:60:6c:
         e0:d3:4a:24:5e:6c:f0:41:0b:60:21:1d:2c:3c:9d:2e:e4:85:
         7f:a7:81:c7:aa:12:37:b1:cc:c9:55:e2:b9:06:1b:9f:0d:87:
         51:e7:75:a4:26:a9:2a:13:16:d3:6a:69:9a:b2:fb:f5:77:8e:
         47:00:8c:76:99:0d:da:3b:f4:49:c0:2a:57:89:30:fb:6d:0f:
         4d:d4:0b:e1:77:bc:a2:28:40:06:28:d0:c2:ad:00:c1:fe:4f:
         18:ff:ac:59:96:08:59:70:eb:a7:c0:97:21:dc:a9:04:ae:ae:
         38:78:e2:7f:ee:9a:30:1b:43:f1:e6:df:86:40:3b:8e:3e:b2:
         b0:0b:0f:f3:bf:df:07:db:a8:27:c6:e8:41:55:3c:f4:dc:84:
         e7:3e:a9:9c:4b:a2:f9:23:28:2e:17:44:56:c1:9c:df:35:91:
         8d:5c:46:9a:71:ea:14:b6:20:04:a6:15:7f:65:8c:01:06:7c:
         9b:85:b8:47:e1:05:9e:e9:02:59:7d:4e:f1:1e:a8:4e:ce:4b:
         7e:bd:c1:e8:d9:2f:39:20:7b:07:03:c8:f2:ac:05:86:d8:e8:
         74:39:9a:7e:18:f0:a7:57:cb:58:d4:52:ec:ff:dd:26:1a:da:
         29:12:d6:7e
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: O=klass.dev Security Domain, OU=pki-tomcat, CN=CA Signing Certificate
        Validity
            Not Before: Jun 10 10:15:36 2019 GMT
            Not After : May 30 10:15:36 2021 GMT
        Subject: O=klass.dev Security Domain, OU=pki-tomcat, CN=CA OCSP Signing Certificate
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:ed:91:c8:5a:33:93:49:83:af:f5:f3:8c:68:d9:
                    b7:23:20:4b:14:65:f3:d1:5f:19:b0:e3:5c:81:e6:
                    fd:24:c1:3c:95:2a:06:b9:34:54:f7:f3:8e:2b:a0:
                    6c:22:a3:f8:19:d1:5c:46:5d:02:4b:39:74:50:a2:
                    58:85:90:7a:5b:21:ba:e0:d6:fa:b6:e3:b2:70:18:
                    68:02:f2:34:15:3f:15:7d:8e:37:58:a1:c9:3a:2e:
                    49:72:cd:f9:e9:0d:de:98:b8:d0:23:fe:45:f3:67:
                    80:ee:fc:10:94:17:2e:54:b9:80:04:82:15:0b:c7:
                    ef:4b:2a:c0:08:ef:ff:a8:b3:da:b4:64:0e:ce:ee:
                    5c:16:92:e8:f0:5f:21:b9:1c:a0:f3:0d:b0:9e:fa:
                    24:3e:03:eb:f1:ae:a2:a8:e7:fa:73:88:3e:e9:53:
                    d9:9e:85:b2:05:76:9a:e0:da:b1:36:90:bb:fd:8c:
                    70:55:4d:c3:f1:c8:85:e2:66:8d:d8:e4:a7:ad:80:
                    d1:d6:c7:f7:91:5f:ab:2b:cd:00:1a:43:75:5e:8a:
                    f1:38:bc:27:1a:88:24:29:7f:1e:3d:6d:f3:d7:5e:
                    6a:59:ba:ff:73:fb:18:77:a8:68:a9:a9:44:62:2d:
                    7e:5a:0d:d3:23:3a:d5:aa:d5:87:92:87:b0:13:c2:
                    0d:17
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:94:A7:33:70:A5:D6:26:B6:64:4D:9A:8D:4B:D9:81:76:17:A7:EA:1E

            Authority Information Access:
                OCSP - URI:http://fedora-ds.klass.dev:8080/ca/ocsp

            X509v3 Extended Key Usage:
                OCSP Signing
            OCSP No Check:

    Signature Algorithm: sha256WithRSAEncryption
         19:90:09:c9:94:59:c1:bd:b2:72:87:3a:20:8d:63:52:cf:66:
         85:28:d6:91:69:ec:8b:e2:de:88:a1:04:35:e7:49:56:2e:cf:
         3c:81:17:60:b0:dc:3e:c6:29:d4:80:bb:05:05:14:46:56:49:
         d4:e5:8a:17:46:43:5f:77:6b:f2:bc:63:9a:18:a0:48:93:35:
         85:38:98:cf:cc:84:a1:fc:a6:9f:47:5d:2c:3a:a2:01:1c:01:
         c4:42:d6:73:c4:24:f9:05:0d:33:e3:f9:2f:cd:09:f0:8a:c5:
         ea:ce:a3:60:07:8b:16:86:06:ec:01:74:09:bd:0a:af:ab:bf:
         9a:ee:fc:2e:8a:a5:44:fb:ce:b0:83:1c:4b:b3:21:50:75:10:
         18:27:93:f0:fc:c2:e9:ba:1f:56:0d:18:a0:be:32:46:7d:bf:
         69:12:72:32:7d:ef:f9:1c:ae:3e:17:eb:f2:db:b9:bb:58:61:
         07:fc:30:94:9c:94:4a:c3:85:4e:f4:36:d3:cc:ac:b4:27:68:
         47:d2:0b:e7:f5:de:36:9a:8d:96:1b:e7:1f:80:cc:e4:f5:2a:
         59:58:ed:6f:a8:8b:a7:5a:d2:43:c6:7c:2d:34:3a:07:71:0d:
         fc:fc:31:f4:df:63:d5:b5:f4:b6:e0:1f:f2:51:78:48:e0:64:
         b6:9e:c6:a6
-----BEGIN CERTIFICATE-----
MIIDxDCCAqygAwIBAgIBAjANBgkqhkiG9w0BAQsFADBaMSIwIAYDVQQKDBlrbGFz
cy5kZXYgU2VjdXJpdHkgRG9tYWluMRMwEQYDVQQLDApwa2ktdG9tY2F0MR8wHQYD
VQQDDBZDQSBTaWduaW5nIENlcnRpZmljYXRlMB4XDTE5MDYxMDEwMTUzNloXDTIx
MDUzMDEwMTUzNlowXzEiMCAGA1UECgwZa2xhc3MuZGV2IFNlY3VyaXR5IERvbWFp
bjETMBEGA1UECwwKcGtpLXRvbWNhdDEkMCIGA1UEAwwbQ0EgT0NTUCBTaWduaW5n
IENlcnRpZmljYXRlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7ZHI
WjOTSYOv9fOMaNm3IyBLFGXz0V8ZsONcgeb9JME8lSoGuTRU9/OOK6BsIqP4GdFc
Rl0CSzl0UKJYhZB6WyG64Nb6tuOycBhoAvI0FT8VfY43WKHJOi5Jcs356Q3emLjQ
I/5F82eA7vwQlBcuVLmABIIVC8fvSyrACO//qLPatGQOzu5cFpLo8F8huRyg8w2w
nvokPgPr8a6iqOf6c4g+6VPZnoWyBXaa4NqxNpC7/YxwVU3D8ciF4maN2OSnrYDR
1sf3kV+rK80AGkN1XorxOLwnGogkKX8ePW3z115qWbr/c/sYd6hoqalEYi1+Wg3T
IzrVqtWHkoewE8INFwIDAQABo4GPMIGMMB8GA1UdIwQYMBaAFJSnM3Cl1ia2ZE2a
jUvZgXYXp+oeMEMGCCsGAQUFBwEBBDcwNTAzBggrBgEFBQcwAYYnaHR0cDovL2Zl
ZG9yYS1kcy5rbGFzcy5kZXY6ODA4MC9jYS9vY3NwMBMGA1UdJQQMMAoGCCsGAQUF
BwMJMA8GCSsGAQUFBzABBQQCBQAwDQYJKoZIhvcNAQELBQADggEBABmQCcmUWcG9
snKHOiCNY1LPZoUo1pFp7Ivi3oihBDXnSVYuzzyBF2Cw3D7GKdSAuwUFFEZWSdTl
ihdGQ193a/K8Y5oYoEiTNYU4mM/MhKH8pp9HXSw6ogEcAcRC1nPEJPkFDTPj+S/N
CfCKxerOo2AHixaGBuwBdAm9Cq+rv5ru/C6KpUT7zrCDHEuzIVB1EBgnk/D8wum6
H1YNGKC+MkZ9v2kScjJ97/kcrj4X6/LbubtYYQf8MJSclErDhU70NtPMrLQnaEfS
C+f13jaajZYb5x+AzOT1KllY7W+oi6da0kPGfC00OgdxDfz8MfTfY9W19LbgH/JR
eEjgZLaexqY=
-----END CERTIFICATE-----
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: O=klass.dev Security Domain, OU=pki-tomcat, CN=CA Signing Certificate
        Validity
            Not Before: Jun 10 10:15:32 2019 GMT
            Not After : Jun 10 10:15:32 2039 GMT
        Subject: O=klass.dev Security Domain, OU=pki-tomcat, CN=CA Signing Certificate
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:dc:3e:a7:65:f7:6b:e1:06:0d:85:8e:0a:d0:7f:
                    9e:24:44:1d:c0:b7:26:2b:2e:76:69:dc:58:b7:e8:
                    ce:23:4f:46:5c:a3:bc:f1:aa:50:16:fa:82:0c:3d:
                    58:38:ff:12:63:3e:bb:df:8d:e9:a5:f2:04:69:e4:
                    1d:76:38:0e:ad:82:39:28:da:56:db:09:47:12:ce:
                    7f:00:b9:be:90:0e:9c:54:56:1a:b1:fa:69:5b:16:
                    87:f9:3f:d2:25:1d:c7:f9:aa:c2:5a:f0:df:53:76:
```

```
                    dd:2c:b5:d1:1c:91:14:ab:d3:34:c8:5c:d1:7c:91:
                    1c:f7:be:04:01:c4:21:6b:ad:dd:6f:f6:00:bf:8d:
                    15:f4:a2:c6:dc:09:d6:2e:1c:f0:4b:e8:80:6f:ae:
                    db:1b:7f:a4:a4:d7:94:10:a1:1a:a5:3d:e6:55:41:
                    b2:5d:77:ff:f3:f9:65:41:3a:93:50:04:33:78:61:
                    dd:03:a5:ff:33:4c:ce:fa:a7:7d:7e:12:25:fa:60:
                    d1:ae:95:64:2e:ed:8e:79:aa:d8:3a:e0:7a:2c:da:
                    aa:b4:90:6f:cd:92:db:0d:ec:f5:51:d9:86:89:7e:
                    01:58:af:74:1a:87:25:c0:4a:ba:e9:c6:82:8f:dd:
                    6d:65:88:53:94:b0:5f:8c:c1:20:e3:be:d8:4b:8b:
                    28:91
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:94:A7:33:70:A5:D6:26:B6:64:4D:9A:8D:4B:D9:81:76:17:A7:EA:1E

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                94:A7:33:70:A5:D6:26:B6:64:4D:9A:8D:4B:D9:81:76:17:A7:EA:1E
            Authority Information Access:
                OCSP - URI:http://fedora-ds.klass.dev:8080/ca/ocsp

    Signature Algorithm: sha256WithRSAEncryption
         bd:22:32:2e:ba:2f:b9:aa:64:7b:9b:86:5e:4b:cc:28:03:ea:
         a4:94:f7:a9:c0:5f:d6:78:9d:8a:71:98:f9:3f:ec:c4:cb:41:
         1a:62:97:6a:67:6e:73:8f:5a:8e:0a:aa:34:b9:40:4e:82:14:
         ab:40:e6:66:71:26:05:25:d5:5f:1c:46:cc:55:df:84:ca:b2:
         4e:b1:1d:b2:e5:51:72:6a:1c:ac:55:00:c9:7a:bb:28:0b:67:
         5a:d6:c3:82:f5:34:17:c1:5a:9a:77:48:21:c0:68:ca:fa:84:
         83:93:3a:10:a8:b3:d9:e6:01:27:20:74:42:d7:bc:68:23:1d:
         4c:82:6a:c0:91:f3:28:88:1c:59:5a:fb:10:d0:40:b4:53:93:
         f9:0f:55:1d:8f:b4:23:fb:6d:f9:16:39:1b:f6:66:49:81:bb:
         05:ad:c2:3d:f3:a5:df:0a:10:1e:93:67:08:2e:45:fb:87:87:
         a9:d6:db:24:8d:d5:40:c8:96:d2:a8:c3:b3:b2:15:19:41:9f:
         d3:b4:ae:e6:89:65:0b:2f:fd:3e:70:8a:79:f9:fc:7f:76:af:
         a3:92:c9:57:90:79:f5:7c:bb:82:73:15:d0:42:96:36:79:3f:
         05:ec:ad:3a:05:8e:5c:df:06:82:28:43:4e:53:b4:bc:24:b7:
         2b:dc:71:0f
-----BEGIN CERTIFICATE-----
MIID2TCCAsGgAwIBAgIBATANBgkqhkiG9w0BAQsFADBaMSIwIAYDVQQKDBlrbGFz
cy5kZXYgU2VjdXJpdHkgRG9tYWluMRMwEQYDVQQLDApwa2ktdG9tY2F0MR8wHQYD
VQQDDBZDQSBTaWduaW5nIENlcnRpZmljYXRlMB4XDTE5MDYxMDEwMTUzMloXDTM5
MDYxMDEwMTUzMlowWjEiMCAGA1UECgwZa2xhc3MuZGV2IFNlY3VyaXR5IERvbWFp
bjETMBEGA1UECwwKcGtpLXRvbWNhdDEfMB0GA1UEAwwWQ0EgU2lnbmluZyBDZXJ0
aWZpY2F0ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANw+p2X3a+EG
DYWOCtB/niREHcC3JisudmncWLfoziNPRlyjvPGqUBb6ggw9WDj/EmM+u9+N6aXy
BGnkHXY4Dq2COSjaVtsJRxLOfwC5vpAOnFRWGrH6aVsWh/k/0iUdx/mqwlrw31N2
3Sy10RyRFKvTNMhc0XyRHPe+BAHEIWut3W/2AL+NFfSixtwJ1i4c8EvogG+u2xt/
pKTXlBChGqU95lVBsl13//P5ZUE6k1AEM3hh3QOl/zNMzvqnfX4SJfpg0a6VZC7t
jnmq2DrgeizaqrSQb82S2w3s9VHZhol+AVivdBqHJcBKuunGgo/dbWWIU5SwX4zB
IOO+2EuLKJECAwEAAaOBqTCBpjAfBgNVHSMEGDAWgBSUpzNwpdYmtmRNmo1L2YF2
F6fqHjAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBxjAdBgNVHQ4EFgQU
lKczcKXWJrZkTZqNS9mBdhen6h4wQwYIKwYBBQUHAQEENzA1MDMGCCsGAQUFBzAB
hidodHRwOi8vZmVkb3JhLWRzLmtsYXNzLmRldjo4MDgwL2NhL29jc3AwDQYJKoZI
hvcNAQELBQADggEBAL0iMi66L7mqZHubhl5LzCgD6qSU96nAX9Z4nYpxmPk/7MTL
QRpil2pnbnOPWo4KqjS5QE6CFKtA5mZxJgUl1V8cRsxV34TKsk6xHbLlUXJqHKxV
AMl6uygLZ1rWw4L1NBfBWpp3SCHAaMr6hIOTOhCos9nmAScgdELXvGgjHUyCasCR
8yiIHFla+xDQQLRTk/kPVR2PtCP7bfkWORv2ZkmBuwWtwj3zpd8KEB6TZwguRfuH
h6nW2ySN1UDIltKow7OyFRlBn9O0ruaJZQsv/T5winn5/H92r6OSyVeQefV8u4Jz
FdBCljZ5PwXsrToFjlzfBoIoQ05TtLwktyvccQ8=
-----END CERTIFICATE-----
Response verify OK
peer.crt: good
        This Update: Jun 12 20:22:11 2019 GMT
```

References:

- https://www.dogtagpki.org/wiki/Quick_Start
- https://www.dogtagpki.org/wiki/DS_Deployment_Scenarios
- https://www.dogtagpki.org/wiki/PKI_Download
- https://www.dogtagpki.org/wiki/CA_Agent_Setup
- https://www.dogtagpki.org/wiki/User_Certificate_Setup
- https://www.dogtagpki.org/wiki/Server_Certificate_Setup
- https://www.dogtagpki.org/wiki/Default_CA_Admin
- https://www.dogtagpki.org/wiki/Certificate_Key_Archival
- https://raymii.org/s/articles/OpenSSL_Manually_Verify_a_certificate_against_an_OCSP.html